PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-303880
(43)Date of publication of application : 13.11.1998

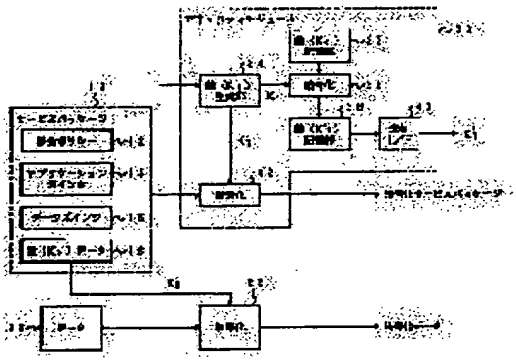
(51)Int.Cl. H04L 9/14
G06F 9/06
G06F 15/00
G09C 1/00
H04L 9/08
H04L 9/10
// H04M 3/42

(21)Application number : 09-113939
(22)Date of filing : 01.05.1997

(71)Applicant : DIGITAL VISION LAB:KK
(72)Inventor : MURATANI HIROBUMI

(54) SERVICE PROVIDING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To maintain the protection function of a service package by sending this package to a user after enciphering it by a 1st encipherment system, enciphering the key of the 1st encipherment system by means of the key stored in an information storage card, sending the ciphered key to the user via an inter-card communication protocol, and decoding the received key in the information storage card by the user.
SOLUTION: The provided data 20 are enciphered by an encipherment part 22 by using a key K2 and sent to a user via a transmitting interface. A service package 10 is also enciphered and sent to the user by using a key K1. The key K1 is enciphered by a key K0 and accordingly both keys K1 and K0 are kept secret to the user and protected. A security module 30 includes a storage part 32 of the key K0, a generation part 34 and encipherment parts 36 and 42 of the key K1, and a storage part 38 and a transmitting interface 40 of an enciphered key K'1 respectively.



LEGAL STATUS
[Date of request for examination] 24.04.1998
[Date of sending the examiner's decision of rejection] 23.07.2002
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection] 2002-16158
[Date of requesting appeal against examiner's decision of rejection] 22.08.2002
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－303880

(43)公開日　平成10年(1998)11月13日

(51)Int.Cl.[6]		識別記号	F.I		
Ｈ０４Ｌ	9/14		Ｈ０４Ｌ	9/00	６４１
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ｚ
	15/00	３３０		15/00	３３０Ｚ
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ａ
Ｈ０４Ｌ	9/08		Ｈ０４Ｍ	3/42	Ｚ

審査請求　有　請求項の数10　ＯＬ　（全９頁）　最終頁に続く

(21)出願番号　特願平9－113939

(22)出願日　平成９年(1997)５月１日

(71)出願人　396001360
株式会社ディジタル・ビジョン・ラボラトリーズ
東京都港区赤坂七丁目３番37号

(72)発明者　村谷　博文
東京都港区赤坂七丁目３番37号　株式会社ディジタル・ビジョン・ラボラトリーズ内

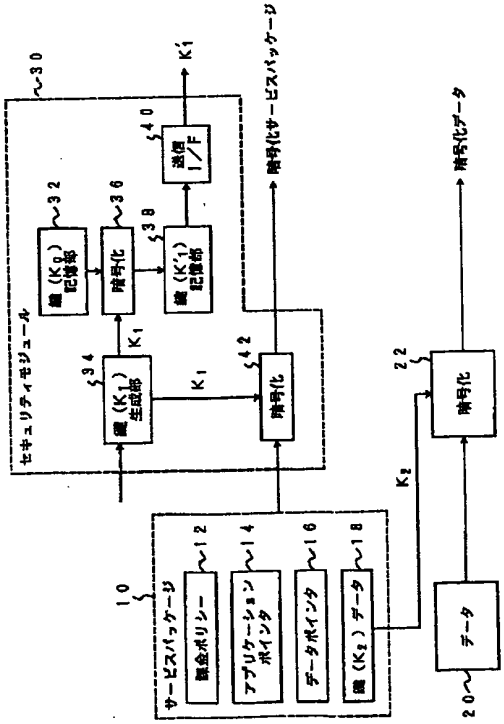
(74)代理人　弁理士　鈴江　武彦　（外５名）

(54)【発明の名称】　サービス提供システム

(57)【要約】

【課題】本発明はサービスパッケージを保護するサービス提供システムに関する。

【解決手段】サービス提供者がサービスパッケージとそれに対応する鍵を生成する。サービスパッケージは暗号化され、利用者に送られる。鍵はすぐにＰＣＭＣＩＡカード内のメモリに記憶される。鍵はサービス提供者から利用者へカード・カード間の通信プロトコルにより安全に伝達される。利用者は鍵を用いてサービスパッケージを利用する。鍵は、利用者のプロセッサ内に留まり、利用者やアプリケーションプログラムに知られることがない。したがって、サービスパッケージのライツが侵害されることがない。また、鍵はロコミのような形で、個人のカードを経由して伝わるので、常駐の鍵発行サーバを設ける必要がない。



1

【特許請求の範囲】

【請求項1】　サービスの利用に必要な情報を記述するサービスパッケージを第1の暗号化方式で暗号化して提供者から利用者へ送り、

提供者は、第1の暗号化方式の鍵を情報記憶カード内で外部へ読み出されないように記憶された鍵を用いて暗号化し、カード・カード間の通信プロトコルで利用者へ送り、

利用者は、暗号化された第1の暗号化方式で使われる鍵を情報記憶カード内で復号化することを特徴とするサービス提供システム。

【請求項2】　復号化されたサービスパッケージの利用者側の端末装置内への保存、及び端末装置から外部への出力が禁止されていることを特徴とする請求項1記載のサービス提供システム。

【請求項3】　暗号化されたサービスパッケージは情報記憶カード内で復号化され、復号化されたサービスパッケージは情報記憶カードの外部へは出力されないことを特徴とする請求項2記載のサービス提供システム。

【請求項4】　前記利用者側の端末装置は、暗号化されたサービスパッケージの復号化手段と、復号化されたサービスパッケージが端末装置内に保存されないこと、及び端末装置外部に出力されないことが保証されていない場合は、サービスパッケージの復号化手段の作動を禁止する手段を具備することを特徴とする請求項2記載のサービス提供システム。

【請求項5】　前記サービスパッケージは提供されるデータを特定する情報、該データを利用するアプリケーションプログラムを特定する情報、該データの利用に関する課金規則を示す情報からなり、

利用者側の端末装置は、復号化されたアプリケーションプログラム特定情報に応じて動作するアプリケーションプログラム実行装置と、復号化された課金規則特定情報に応じて動作する課金処理装置と、データの転送を制御するデータ転送処理部からなることを特徴とする請求項1記載のサービス提供システム。

【請求項6】　前記アプリケーションプログラム実行装置はアプリケーションプログラムにより実現され、前記課金処理装置はアプリケーションプログラムとは異なるプラットフォームにより実現されることを特徴とする請求項5記載のサービス提供システム。

【請求項7】　暗号化されたサービスパッケージ内の課金規則と同じ内容の第2の課金規則を暗号化しないで提供者から利用者へさらに送ることを特徴とする請求項5記載のサービス提供システム。

【請求項8】　前記第1の暗号化方式で使われる鍵は情報記憶カード内で生成され、カード外部には出力されないように情報記憶カードに保存されることを特徴とする請求項1記載のサービス提供システム。

【請求項9】　サービスパッケージを特定する情報とサービスパッケージの暗号化に使われる鍵を特定する情報とを対応づけるチケットもカード・カード間の通信プロトコルで提供者から利用者へ送り、

利用者はチケットから利用するサービスパッケージに対応する鍵を特定することができることを特徴とする請求項1記載のサービス提供システム。

【請求項10】　サービスの利用に必要な情報を記述するサービスパッケージを第1の暗号化方式で暗号化して提供者から利用者へ送り、

提供者は、第1の暗号化方式の鍵をセキュリティモジュール内で外部へ読み出されないように記憶された鍵を用いて暗号化し、利用者のセキュリティモジュールへ送り、

利用者は、暗号化された第1の暗号化方式で使われる鍵をセキュリティモジュール内で復号化することを特徴とするサービス提供システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は提供する情報サービス（データ）の保護を図りつつ、データの流通を推進するサービス提供システムに関する。

【０００２】

【従来の技術】インターネットの進歩やＤＶＤ等の大容量記憶媒体の発達により、オンライン、オフラインを問わず、種々の情報提供サービスが行われている。サービス提供者は、利用者に課金して利用料を徴収することにより、事業としてサービス提供を行うことができる。

【０００３】課金の形態として、サービスを受けている時間に応じた課金、サービスを受けたデータ量（バイト）に応じた課金、パッケージ（例えば映画1本）毎の一括課金等、無限に近い種々の形態があるが、現状では、サービス提供者が予め決めた課金形態のみが実施されている。具体的には、ケーブルテレビジョン放送サービスのように専用のハードウェアを用いるクローズドシステムにおいては、利用者が所有するデータ処理端末（データを利用するコンピュータ等）、あるいはサービス提供者が所有するサーバに組み込まれているアプリケーションプログラム中に課金処理プログラムが記載されている。このため、課金形態を変更するには、アプリケーションプログラム自体を書き直す必要があり、簡単には課金形態を変更することができない。同様に、多様性を持たせるために、新たな課金形態（単数でも複数でも可）を追加し、いずれかの課金形態を選択できるようにすることも望ましいが、プログラムの大幅変更が必要であり、簡単にはできない。

【０００４】また、近年のマルチメディアの発達に伴い、１人の利用者がインターネットを介して多数のサービス提供者と契約して、多数のサービスを受けることも増えてきている。この場合、個々のサービス毎にアプリケーションプログラムが必要となる。従来の課金処理機

3

能はアプリケーションプログラムに含まれているので、異なる言語のアプリケーションプログラムには適用できない。そのため、サービス提供者が新たなアプリケーションプログラムを作成すると、課金処理プログラムも新たに作成する必要がある。しかし、課金処理機能は、本来、アプリケーションプログラムとは独立しており、異なるアプリケーションプログラムに対して共通に使えるはずであり、各アプリケーションプログラム毎に課金処理プログラムを用意するのは、プログラム開発時間が無駄であるとともに、プログラムサイズが大きく、複雑になる欠点がある。

【０００５】そこで、オープンなシステムにおいて、情報の利用と課金処理とを分離し、情報の利用（データ処理機能）はアプリケーションプログラムにより実現し、課金機能はアプリケーションプログラムとは異なるプラットフォームにより実現することを本発明者は先に提案した（特願平８－２５９４３３号）。ここでは、サービス提供者は提供するサービス（データ、コンテンツ）、あるいはサービスを特定するアドレス等の情報と、そのサービスを制御するのに必要なサービス固有の制御情報（サービス記述と称する）とを分離し、両者を対にしたサービスパッケージを生成する。サービス記述とは、提供されるサービスを利用するアプリケーションプログラムの特定、該サービスの利用に係る課金ポリシーの特定のための情報、暗号化されているサービスの復号化に必要な鍵を示す情報を含む。例えば、映像データ乙を処理するにはビデオ再生用のアプリケーションプログラムが必要であり、利用料は１０００円／１本であるということがサービス記述である。このように、利用者サイトでは、サービス記述を基にサービスを利用することができる。

【０００６】サービス提供者から利用者までの情報伝達経路、または利用者サイトにおいて、このサービスパッケージが保護されていない状態に置かれると、サービス記述の改竄等により正当な利用料を徴収できなくなったり、コンテンツの保護が破られたりして、サービスのライツが保護されない状態になる。

【０００７】サービスのライツとしては、コンテンツ／データの著作権とともにサービス記述の権利も含まれる。例えば、サービスを制作した人がその情報を「どのように利用して欲しい」、「どのような利用はして欲しくない」等、主張できる権利である。例えば、コンピュータプログラムを書いた人が「本プログラムは実行してもよいが、コピーは禁止する」、あるいは「コピーしてもよいが、変更は禁止する」ということを主張したり、課金ポリシーとして「利用料は１０円／１分」等をサービス記述として規定することができる。サービス記述に従わない利用はライツの侵害である。サービスパッケージが保護されていないと、悪意の利用者により課金ポリシーが書換えられ、利用料を無料とされてしまう。この

4

場合、課金処理用のプロセッサが働かずに、サービス提供者が損害を被ってしまう。

【０００８】このため、ライツを保護するには、提供するコンテンツの保護とともにサービス記述の保護が必要である。サービス記述もコンテンツと同じディジタルデータであるので、暗号化して保護することが考えられる。すなわち、サービスの利用に際して、サービス提供者から発行されたトークンやチケット等の鍵が無いとコンテンツ、およびサービス記述の内容を解釈できないようにしておく。鍵はサービスパッケージとは別途、保護されている安全な経路でサービス提供者から利用者へ伝達される。

【０００９】図1はこのような従来例の構成を示すブロック図である。提供者側の端末装置1は、データ３を暗号化部4で暗号化してから利用者側の端末装置2へ送る。暗号化の鍵は鍵発生部6で発生され、鍵管理部5により、暗号化データとは別に安全な経路で利用者側端末装置2へ送られる。利用者側では、鍵が鍵管理部8に格納され、暗号化データが復号化部7に格納される。鍵管理部8内の鍵を用いて復号化部7でデータが復号化され、データ９が利用に供される。

【００１０】しかし、いくら鍵を安全な経路で利用者へ送っても、鍵を利用者や利用者のアプリケーションプログラムに渡してしまうと、利用者サイトにおいて復号後のサービス記述を改竄できる余地があり、やはりサービスのライツの保護が出来なくなる本質的な欠点がある。

【００１１】また、サービスパッケージやコンテンツ自体を、放送、オンデマンド、ＤＶＤ等の種々のコンテンツの伝達形態に依存しない形で暗号化して利用者に渡すとしても、鍵はオンデマンドで渡すため、何時、サービスの要求があるか分からないので、サービス提供者は常に鍵発行サーバ（鍵管理部5）を作動させておく必要がある。これは、サービス提供のコストがかかるので、個人による情報発信には向かない。

【００１２】【発明が解決しようとする課題】このように従来のサービス提供システムは、課金処理等のサービス実現に必要な機能をプラットフォーム化するために、課金等に関するサービス記述と提供するデータとを別々に管理する場合、サービス記述の保護が不十分であり、サービスパッケージの保護ができない、サービス提供者のライツを守れない等の欠点がある。また、これに対処するために、サービス提供者側の鍵発行サーバを常時作動させておくことは、個人が情報発信するには向かないという欠点がある。

【００１３】本発明の目的は次のようなサービス提供システムを提供することにある。サービスの流通を図りつつ、サービス提供者から利用者までの伝達経路も含めて利用者サイトにおけるサービスパッケージの保護機能を持つ。

5

【００１４】
【課題を解決するための手段】前記課題を解決し目的を達成するために、本発明は以下に示す手段を用いている。本発明の第1 態様に係るサービス提供システムは、サービスの利用に必要な情報を記述するサービスパッケージを第1 の暗号化方式で暗号化して提供者から利用者へ送り、提供者は、第1 の暗号化方式の鍵を情報記憶カード内で外部へ読み出されないように記憶された鍵を用いて暗号化し、カード・カード間の通信プロトコルで利用者へ送り、利用者は、暗号化された第1 の暗号化方式で使われる鍵を情報記憶カード内で復号化することを特徴とする。
【００１５】本発明の第2 態様に係るサービス提供システムは、第1 態様において、復号化されたサービスパッケージの利用者側の端末装置内への保存、及び端末装置から外部への出力が禁止されていることを特徴とする。
【００１６】本発明の第3 態様に係るサービス提供システムは、第2 態様において、暗号化されたサービスパッケージは情報記憶カード内で復号化され、復号化されたサービスパッケージは情報記憶カードの外部へは出力されないことを特徴とする。
【００１７】本発明の第4 態様に係るサービス提供システムは、第2 態様において、前記利用者側の端末装置は、暗号化されたサービスパッケージの復号化手段と、復号化されたサービスパッケージが端末装置内に保存されないこと、及び端末装置外部に出力されないことが保証されていない場合は、サービスパッケージの復号化手段の作動を禁止する手段を具備することを特徴とする。
【００１８】本発明の第5 態様に係るサービス提供システムは、第1 態様において、前記サービスパッケージは提供されるデータを特定する情報、該データを利用するアプリケーションプログラムを特定する情報、該データの利用に関する課金規則を示す情報からなり、利用者側の端末装置は、復号化されたアプリケーションプログラム特定情報に応じて動作するアプリケーションプログラム実行装置と、復号化された課金規則特定情報に応じて動作する課金処理装置と、データの転送を制御するデータ転送処理部からなることを特徴とする。
【００１９】本発明の第6 様に係るサービス提供システムは、第5 態様において、前記アプリケーションプログラム実行装置はアプリケーションプログラムにより実現され、前記課金処理装置はアプリケーションプログラムとは異なるプラットフォームにより実現されることを特徴とする。
【００２０】本発明の第7 態様に係るサービス提供システムは、第5 態様において、暗号化されたサービスパッケージ内の課金規則と同じ内容の第2 の課金規則を暗号化しないで提供者から利用者へさらに送ることを特徴とする。
【００２１】本発明の第8 態様に係るサービス提供システムは、第1 態様において、前記第1 の暗号化方式で使われる鍵は情報記憶カード内で生成され、カード外部には出力されないように情報記憶カードに保存されることを特徴とする。
【００２２】本発明の第9 態様に係るサービス提供システムは、第1 態様において、サービスパッケージを特定する情報とサービスパッケージの暗号化に使われる鍵を特定する情報とを対応づけるチケットもカード・カード間の通信プロトコルで提供者から利用者へ送り、利用者はチケットから利用するサービスパッケージに対応する鍵を特定することができることを特徴とする。
【００２３】本発明の第１０態様に係るサービス提供システムは、サービスの利用に必要な情報を記述するサービスパッケージを第1 の暗号化方式で暗号化して提供者から利用者へ送り、提供者は、第1 の暗号化方式の鍵をセキュリティモジュール内で外部へ読み出されないように記憶された鍵を用いて暗号化し、利用者のセキュリティモジュールへ送り、利用者は、暗号化された第1 の暗号化方式で使われる鍵をセキュリティモジュール内で復号化することを特徴とする。
【００２４】
【発明の実施の形態】以下、図面を参照して本発明によるサービス提供システムの実施形態を説明する。図2 は本発明の第1 実施形態に係る提供者側の端末装置の構成を示す図である。本発明でも、従来の技術で説明したように、課金処理機能をプラットフォーム化するために、情報提供サービスが提供するデータ(の名前) とそのサービスの制御に必要な情報(サービス記述と称する) を対にしたもの、あるいは、その対応関係を表わす情報をサービスパッケージ１０としてサービス提供者側のデータ処理装置(サーバ等) が生成する。サービスパッケージの一例は、MPEGデータ「１」(サービスが提供するデータの名前、あるいはそのデータのアドレス) を鍵「Ｋ２」で復号化し、アプリケーションプログラム「ａ」で処理し、課金処理「甲」を行うというようなものである。利用者側ではサービスパッケージ１０のサービス記述を基に実際にサービスを実現し、利用することができる。このため、サービスパッケージ１０は課金形態を示す課金ポリシー１２、データを利用するアプリケーションプログラムを示すアプリケーションポインタ１４、提供されるデータの名前、あるいはそのアドレスを示すデータポインタ１６、データの復号化に必要な鍵Ｋ２を示す鍵データ１８からなる。
【００２５】提供されるデータ２０は鍵Ｋ２を用いて暗号化部２２で暗号化され、図示しない送信インターフェースを介して暗号化データとして利用者サイトへ送られる。暗号化の鍵Ｋ２は提供者が自由に選ぶことができるが、データ固有の鍵とすることが好ましい。暗号化データは、インターネット等でオンラインで配布してもよいし、ＤＶＤ等を用いてオフラインで配布してもよい。

7

【００２６】暗号化は共通鍵方式でも、公開鍵方式でもよい。共通鍵方式では、データの暗号化に用いられる鍵と、暗号データの復号化に用いられる鍵とが同一である方式である。一方、公開鍵方式は暗号化の鍵と復号化の鍵とが異なり、いずれか一方を公開し、他方は秘密とする。提供者は利用者の公開鍵を用いてデータを暗号化する。利用者はその暗号データを自分の秘密鍵を用いて復号化する。そのため、公開鍵方式の暗号化は利用者が特定されている場合のみ採用でき、これを採用する場合は、暗号化鍵Ｋ２を利用者へ送る必要がないので、サービスパッケージ１０に鍵Ｋ２を含める必要はない。なお、共通鍵方式の暗号化を採用する場合でも、鍵Ｋ２は必ずしも本発明により保護されているサービスパッケージ１０内に含める必要はなく、別途安全な経路があれば、それを介して利用者へ送ってもよい。

【００２７】サービスパッケージ１０自身も暗号化されて、利用者サイトへ送られる。この送信も、オンラインでもオフラインでも構わない。だたし、サービスパッケージの暗号化はデータの暗号化鍵Ｋ２とは別の鍵Ｋ１を用いて行われ、この鍵Ｋ１自体も更に別の鍵Ｋ０を用いて暗号化されて、利用者サイトへ送られる。これらのサービスパッケージ１０の暗号化、暗号化鍵の暗号化も共通鍵方式に限らず、利用者が特定されている場合は公開鍵方式を採用してもよい。

【００２８】そして、鍵Ｋ１自身、及び鍵Ｋ１の暗号化のための鍵Ｋ０は絶対に利用者に知られないようになっている。このため、本発明では、外部へデータが読み出されることが物理的に禁止されているセキュリティモジュール３０が用いられ、暗号化はこのモジュール３０内で行われる。モジュール３０としては、データが物理的に保護されている半導体情報記憶カード（ＩＣカード、ＰＣＭＣＩＡカード等）等を利用することが、端末装置の汎用性を高める上で好ましいが、端末装置が専用端末装置として実現される場合は、カード等の着脱自在な構成にする必要はなく、装置の一部に固定的に実装されるものでもよい。

【００２９】セキュリティモジュール３０は、鍵Ｋ０の記憶部３２、鍵Ｋ１の生成部３４、暗号化部３６、４２、暗号化された鍵Ｋ１'の記憶部３８、暗号化された鍵Ｋ１'の送信インターフェース４０を具備する。鍵Ｋ１の生成部３４は、外部から供給されたサービスパッケージ１０を特定する情報に応じてサービスパッケージ固有の暗号化鍵Ｋ１を生成する。しかし、この鍵Ｋ１は必ずしも、モジュール３０内で生成する必要はなく、信頼のおける機関が生成し、外部からアクセスされることなくセキュリティモジュール３０内に書き込んでもよい。

【００３０】サービスパッケージ１０は暗号化部４２で鍵Ｋ１により暗号化され、図示しない送信インターフェースを介して利用者サイトへ送られる。サービスパッケージ１０の暗号化に用いられた鍵Ｋ１は暗号化部３６でセキュリティモジュール３０内に格納されている鍵Ｋ０により暗号化される。この鍵Ｋ０の記憶部３２は不揮発性メモリからなり、鍵Ｋ０はカードを作成した時に格納され、その後、外部からは絶対にアクセスできないようになっている。鍵Ｋ０は、データ／サービスパッケージに関わりなく、提供者に固有の鍵でよい。

8

【００３１】暗号化された鍵Ｋ１'は一旦記憶部３８に格納される。これは、同一のサービスパッケージの暗号化の際に、その都度、鍵Ｋ１を暗号化する作業を省略できるためである。そのため、鍵Ｋ１'記憶部３８は複数のサービスパッケージの暗号化鍵Ｋ１を鍵Ｋ０で暗号化した鍵Ｋ１'を格納でき、サービスパッケージが特定されると、既に格納している鍵Ｋ１'の中に当該サービスパッケージに対応する鍵がある場合は、それを読み出す。

【００３２】記憶部３８内の鍵Ｋ１'は外部からアクセスされることなく利用者のセキュリティモジュールへ送られる。半導体情報記憶カードがセキュリティモジュールとして用いられる場合は、カード・カード間の通信プロトコルにより、利用者のカードへ鍵Ｋ１'が安全に送られる。このように、サービスパッケージの暗号化鍵Ｋ１を暗号化した鍵Ｋ１'がセキュリティモジュール以外に出力されることが無く、利用者に知られることがないので、第３者のサービスパッケージの改竄を防ぐことができる。

【００３３】なお、暗号化された暗号鍵Ｋ１'の伝達は、暗号化サービスパッケージの伝達と同時でなくても構わない。しかし、上述したように鍵Ｋ１はサービスパッケージ固有であるので、利用者側に、複数の暗号化サービスパッケージと暗号化された暗号鍵Ｋ１'が存在する場合、両者の対応関係が不明であると、復号化できない。このため、図示してはいないが、提供者側からサービスパッケージを特定する情報とサービスパッケージの暗号化に用いられた鍵Ｋ１を特定する情報とを対応づける情報（これをチケットと称する）を提供者から利用者へ送ることが望ましい。こうすれば、利用者はチケットから利用したいサービスパッケージに対応する鍵Ｋ１を特定することができる。

【００３４】図３は利用者側の端末装置の構成を示す図である。利用者側も、例えば半導体情報記憶カードからなるセキュリティモジュール５０を使用する。セキュリティモジュール５０は受信インターフェース５２、復号化部５４、６０、鍵Ｋ０の記憶部５６、鍵Ｋ１の記憶部５８、サービス実行部６２を有する。

【００３５】利用者は提供者からセキュリティモジュールどうしの安全な通信で暗号鍵Ｋ１'を受け取る。このため、契約していない利用者に鍵Ｋ１'が送られることがない。暗号鍵Ｋ１'は受信インターフェース５２を介して復号化部５４に供給される。利用者側のセキュリティモジュール５０にも提供者側のセキュリティモジュール３０と同様に暗号鍵Ｋ０の記憶部５６を有する。この鍵Ｋ０

の記憶部56も不揮発性メモリからなり、鍵K0はカードを作成した時に格納され、その後、外部からは絶対にアクセスできないようになっている。そのため、提供者側で鍵K0を用いて暗号化されたサービスパッケージの暗号化鍵K1'を利用者側で復号化できる。なお、ここでも、公開鍵方式の暗号化を採用してもよい。復号化された鍵K1は一旦記憶部58に格納される。これも、同一のサービスパッケージの復号化の際に、その都度、鍵K1'を復号化する作業を省略するためである。また、記憶部58の複数のサービスパッケージに対応する鍵K1を記憶することができる。

【0036】一方、暗号化サービスパッケージは受信インターフェース64を介してサービスパッケージ記憶部66に一旦記憶され、暗号化データは受信インターフェース68を介してデータ記憶部70に一旦記憶される。サービスパッケージはセキュリティモジュール50内の復号化部60で記憶部58に格納されている鍵K1を用いて復号化され、サービス実行部62に供給される。なお、サービスパッケージに含まれる鍵K2はセキュリティモジュール50から出力され、復号化部72に供給される。復号化部72は記憶部70に格納されている暗号化データを鍵K2を用いて復号化し、データ再生部(例えば、表示部)74に供給され、サービスの利用が行われる。

【0037】利用者側の端末装置は、ユーザインターフェース76と、サービス制御部78も具備し、サービス制御部78は鍵K1の記憶部58、サービスパッケージ記憶部66、サービス実行部62を制御する。

【0038】図4はサービス実行部62の具体的な構成を示す図である。サービス実行部62は、課金ポリシー12に基づいて課金処理を行う課金処理モジュール82と、アプリケーションポインタ14、データポインタ16に基づいて実行されるアプリケーションプログラム84と、課金処理モジュール82、アプリケーションプログラム84とともにデータ88の取込みを行うデータ転送処理モジュール86とを具備する。このようにサービス実現部62は、サービス記述に基づいてサービス実現のために必要なハードウェア、ソフトウェア、それらを作動させるためのパラメータ等からなり、サービス実現のために必要な機能の集合である。

【0039】第1実施形態の動作を説明する。利用者は提供者から頒布された鍵K0記憶部56を有するセキュリティモジュール50を使用することが前提となっている。暗号化サービスパッケージ、暗号化データはインターネット等のオンラインで、あるいはDVD等の大容量記憶媒体を介してオフラインで、すなわち任意の形態で利用者側に伝達しておく。利用者はサービスを利用したい場合、提供者からサービスパッケージ固有の鍵K1'を貰う。この鍵K1'を受け取ったセキュリティモジュール50を端末装置に装着し、暗号化サービスパッケージを復号化し、サービスパッケージからサービスインスタンスを生成する。とともに、サービスパッケージに含まれている鍵K2を用いて暗号化データを復号化する。

【0040】復号化されたサービスパッケージのうち、アプリケーションポインタ14、データポインタ16は所定のアプリケーションプログラム84を起動する。これに連動して、データ転送処理モジュール86は該当するデータ88をサーバ、記憶媒体から読み出し、利用を開始する。サービスの利用に応じて、課金ポリシーに従った課金処理が課金処理モジュール82で行われる。

【0041】このように本実施形態によれば、データとサービスパッケージが別々の暗号化鍵で暗号化され、利用者に送られる。ここで、サービスパッケージの暗号化に使われた鍵は、更に別の鍵を用いて暗号化され、利用者に送られる。この鍵の暗号化に使われる別の鍵は外部から読み出し不可能なセキュリティモジュール内の記憶部に格納され、暗号化された鍵も外部に読み出されない状態でセキュリティモジュール間のみで直接送られる。このため、利用者やそのアプリケーションプログラムがサービスパッケージを書換えることは出来ない。そのため、課金ポリシー等を改竄して不正な利用をすることを防止できる。

【0042】本発明は上述した実施形態に限定されるものではなく、種々変形して実施可能である。例えば、図2、図3では必要最低限の回路しかセキュリティモジュール内に内蔵していないが、セキュリティモジュールに余裕がある場合は、提供するデータ20の暗号化部22、復号化部72もセキュリティモジュール30、50に内蔵してもよい。

【0043】また、提供者側のセキュリティモジュール30と利用者側のセキュリティモジュール50とを同一の構成としてもよい。この場合の一例を図5に示す。鍵(K0)記憶部100が暗号化／復号化部102に接続され、暗号化／復号化部102に鍵(K1)記憶部106、鍵(K1')記憶部108が接続される。鍵(K1')記憶部108には送受信インターフェース110が接続される。サービスパッケージを特定する情報が鍵(K1)生成部104に与えられ、当該サービスパッケージの暗号化に用いられる鍵K1が生成され、鍵記憶部106に格納される。鍵K1はサービスパッケージ暗号化／復号化部112に供給される。サービスパッケージ暗号化／復号化部112には送受信インターフェース114、サービスインスタンス生成部116が接続される。

【0044】このモジュールを提供者が使う場合は、サービスパッケージ固有の鍵K1を生成し、サービスパッケージ暗号化／復号化部112によりサービスパッケージを暗号化して送受信インターフェース114を介して暗号化サービスパッケージを送信する。とともに、鍵K1を鍵K0を用いて暗号化／復号化部102により暗号化し、送受信インターフェース110を介して暗号化し

11

た鍵K１'を介して送信する。

【００４５】このモジュールを利用者が使う場合は、送受信インターフェース１１０を介して提供者から受け取った暗号化されている鍵K１'を鍵K０を用いて暗号化／復号化部１０２により復号化し、鍵（Ｋ１）記憶部１０６に格納する。送受信インターフェース１１４を介して受け取った暗号化サービスパッケージを鍵Ｋ１を用いてサービスパッケージ暗号化／復号化部１１２により復号化し、サービスインスタンス生成部１１６に供給する。

【００４６】このような構成によれば、提供者、利用者ともに同一のセキュリティモジュールを使用でき、コスト低減に効果がある。なお、この場合も、セキュリティモジュールのハードウェアに余裕があれば、データの暗号化／復号化部もモジュールに内蔵してもよい。また、利用者が提供者と同一構成のセキュリティモジュールを所持していれば、サービスパッケージの暗号化に使われる鍵K１'を提供者が直接に利用者に送信する必要はなく、利用者も他の利用者へ鍵K１'を送信することができ、中間に複数の利用者のセキュリティモジュールを経由して鍵K１'を送信することもできる。こうすると、鍵は「口コミ」のような形で個人から個人へ伝達していき、鍵発行用のサーバを常時作動させる必要がなく、個人による情報発信に好適である。この場合、鍵を中継するだけの者は、図5の構成を全部必要とするわけではなく、鍵（Ｋ１'）記憶部１０８、送受信インターフェース１１０のみあればよい。しかし、公開鍵方式を用いる場合は、中継者サイトで鍵K１'の暗号化を一旦解かなければならないので、図5の構成のうち、省略できるのは、サービスパッケージ暗号化／復号化部１１２、送受信インターフェース１１４、サービスインスタンス１１６だけである。

【００４７】上述の説明では、復号化されたサービスパッケージを利用者に知られないようにするために、復号化部６０及びサービス実行部６２をセキュリティモジュール５０内に設け、ハードウェア的に情報の改竄を防いでいるが、ソフトウェア的にサービスパッケージを保護してもよい。サービスパッケージを実行するためのソフトウェアであるサービスインスタンス自体にサービスパッケージ、鍵Ｋ１を外部に出力しない、保存しないことを保証させる認証を付加し、この認証が無い場合は、サービスパッケージの復号化を禁止するようにしてもよい。この場合は、復号化部６０及びサービス実行部６２をセキュリティモジュール５０内に設ける必要はない。また、ハードウェア的に情報の改竄を防ぐ場合でも、利用者側の端末装置が信頼のおけるものである場合は、復号化部６０、サービス実現部６２をセキュリティモジュール５０内に設けなくてもよい。

【００４８】また、サービスパッケージの復号／課金処理系をプラットフォームとしたが、通常のデータ処理機能と同じアプリケーションプログラムにより実現しても

12

よい。

【００４９】さらに、上述の説明では、利用者が課金ポリシーを見るには、必ず復号化する必要があり、復号化のためにはセキュリティモジュールが必要であったが、利用する前は利用者はセキュリティモジュールを所持していないので、これでは不便である。そのため、サービスパッケージ１０として暗号化して送信する課金ポリシー１２と同じ内容の第2の課金ポリシーを別途用意し、これは暗号化しないで利用者サイトへ送るようにする。利用者はこの第2の課金ポリシーを読んで、このサービスを利用するか否かを決めることができる。この場合、サービス実現部６２に供給されるのは、当然、復号化されたサービスパッケージに含まれている課金ポリシーである。しかし、平文の第2の課金ポリシーを第3者が改竄して、本来有料のものを無料と騙すおそれがあり、このままでは、利用者の保護に欠けるので、利用者側の端末装置は、復号化された課金ポリシーと第2の課金ポリシーとを比較して、不一致の場合は利用を禁止する手段を設けることが望ましい。

【００５０】

【発明の効果】以上説明したように本発明によれば、サービス提供者から利用者までの伝達経路も含めて利用者サイトにおけるサービスパッケージの保護機能を持つサービス提供システムを提供することができる。

【図面の簡単な説明】

【図1】サービス提供システムの従来例の構成を示すブロック図。

【図2】本発明によるサービス提供システムの第1実施形態における提供者側のシステム構成を示すブロック図。

【図3】本発明によるサービス提供システムの第1実施形態における利用者側のシステム構成を示すブロック図。

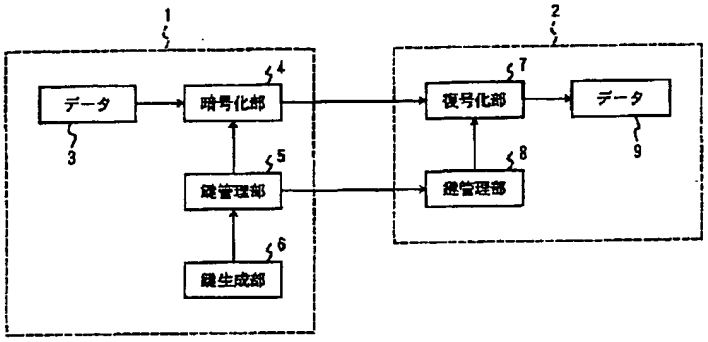
【図4】図3のサービスインスタンスの詳細なブロック図。

【図5】本発明のサービス提供システムの第2実施形態におけるセキュリティモジュールの構成を示すブロック図。

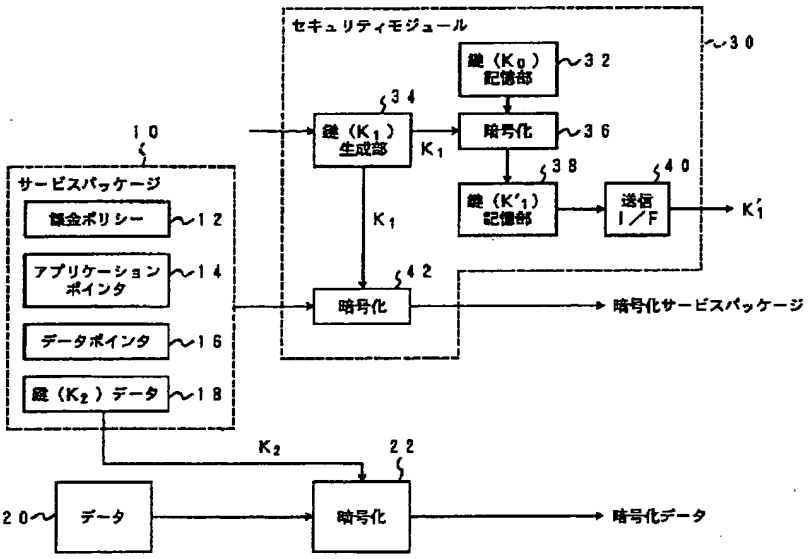
【符号の説明】

１０…サービスパッケージ
１２…課金ポリシー
１４…アプリケーションポインタ
１６…データポインタ
２２、３６…暗号化部
３０、５０…セキュリティモジュール
３２、３８、５６、５８…鍵記憶部
３４…鍵生成部
５４、６０…復号化部
６２…サービスインスタンス

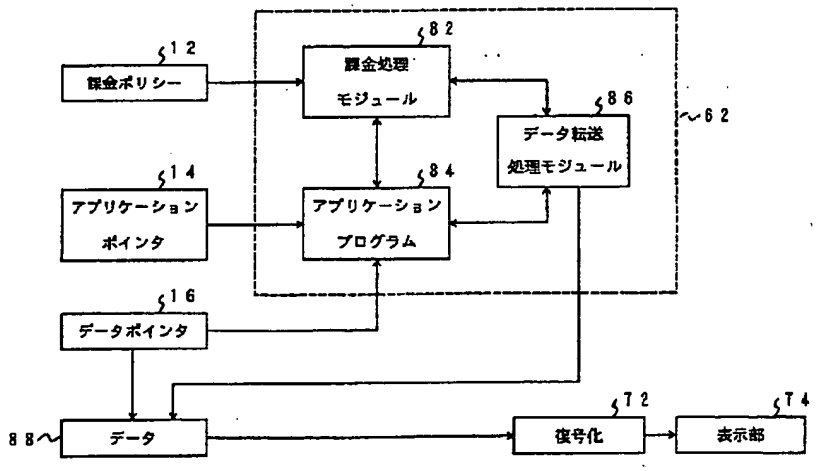
【 図1 】


1
2
データ
3
暗号化部
4
鍵管理部
5
鍵生成部
6
復号化部
7
鍵管理部
8
データ
9

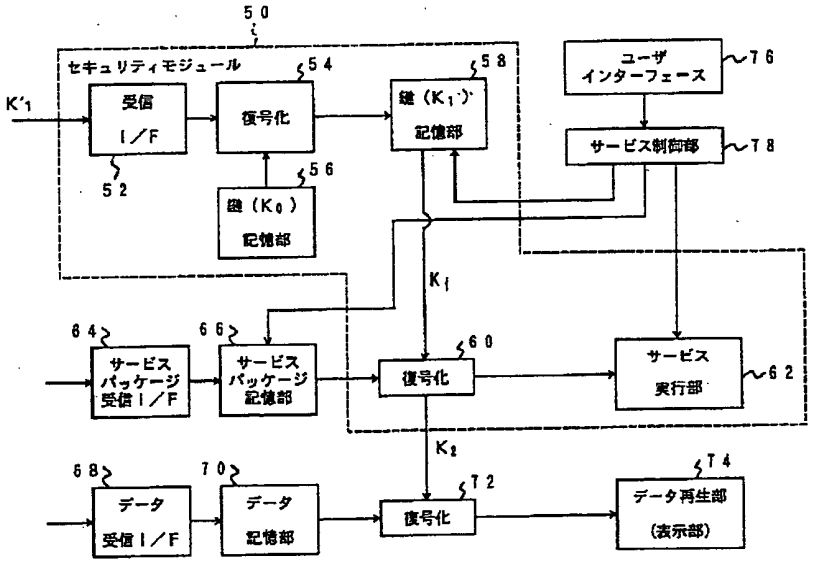
【 図2 】


セキュリティモジュール
30
鍵（K0）記憶部
32
鍵（K1）生成部
34
K1
暗号化
36
鍵（K'1）記憶部
38
送信I／F
40
K'1
K1
暗号化
42
暗号化サービスパッケージ
10
サービスパッケージ
課金ポリシー
12
アプリケーションポインタ
14
データポインタ
16
鍵（K2）データ
18
K2
22
20
データ
暗号化
暗号化データ

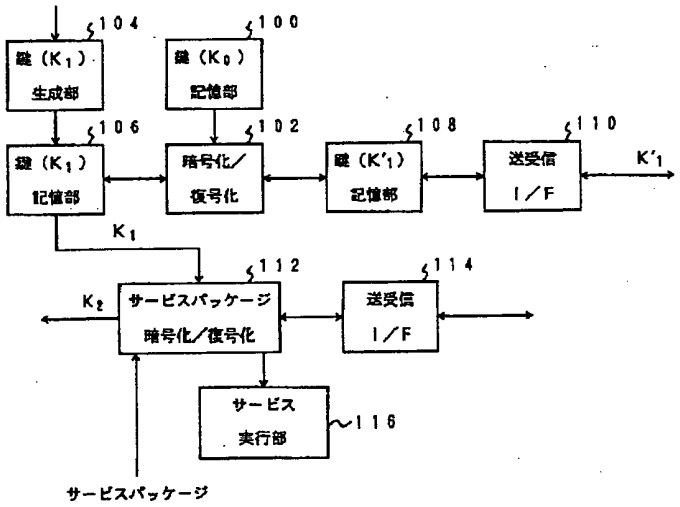
【 図4 】


課金ポリシー
12
課金処理モジュール
82
データ転送処理モジュール
86
62
アプリケーションポインタ
14
アプリケーションプログラム
84
データポインタ
16
88
データ
復号化
72
表示部
74

【 図3 】



【 図5 】



フロントページの続き

(51)Int.Cl.⁶		識別記号	FI		
H04L	9/10		H04L	9/00	601A
// H04M	3/42				621A